DATA GOVERNANCE AND MASTER DATA MANAGEMENT CONFERENCE EUROPE

11 - 14 March 2024 | London, UK

Please score and comment on this session and speaker in the event mobile app

IRMUK

TECHNOLOGIES
Bring the future to humanity

How to prepare for the EU AI Regulations

Director, Chief AI Officer, PhD
AI Technologies

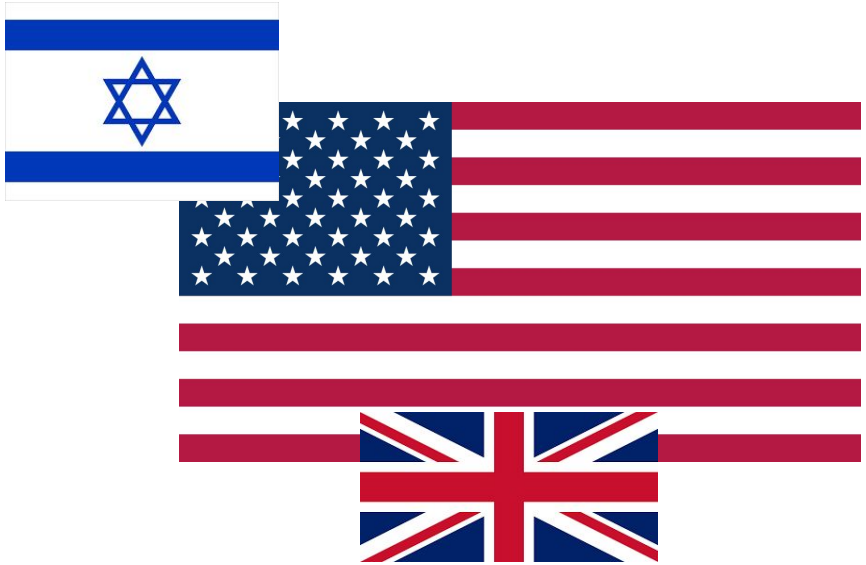
TECHNOLOGIES
Bring the future to humanity

REASONS FOR THIS TALK

- ✔ Overview on the AI incoming regulations
- ✔ Impacts on the AI technical team when the governance is implemented
- ✔ Hints and suggestions on how to structure a good AI model governance
- ✔ Certifications standards on AI models: what to do
- ✔ Overview on how to combine the data governance and the new AI governance

Global view on regulations

EU AI regulations are coming by 2024



Relaxing rules

Regulating

Banning

OECD

ISO

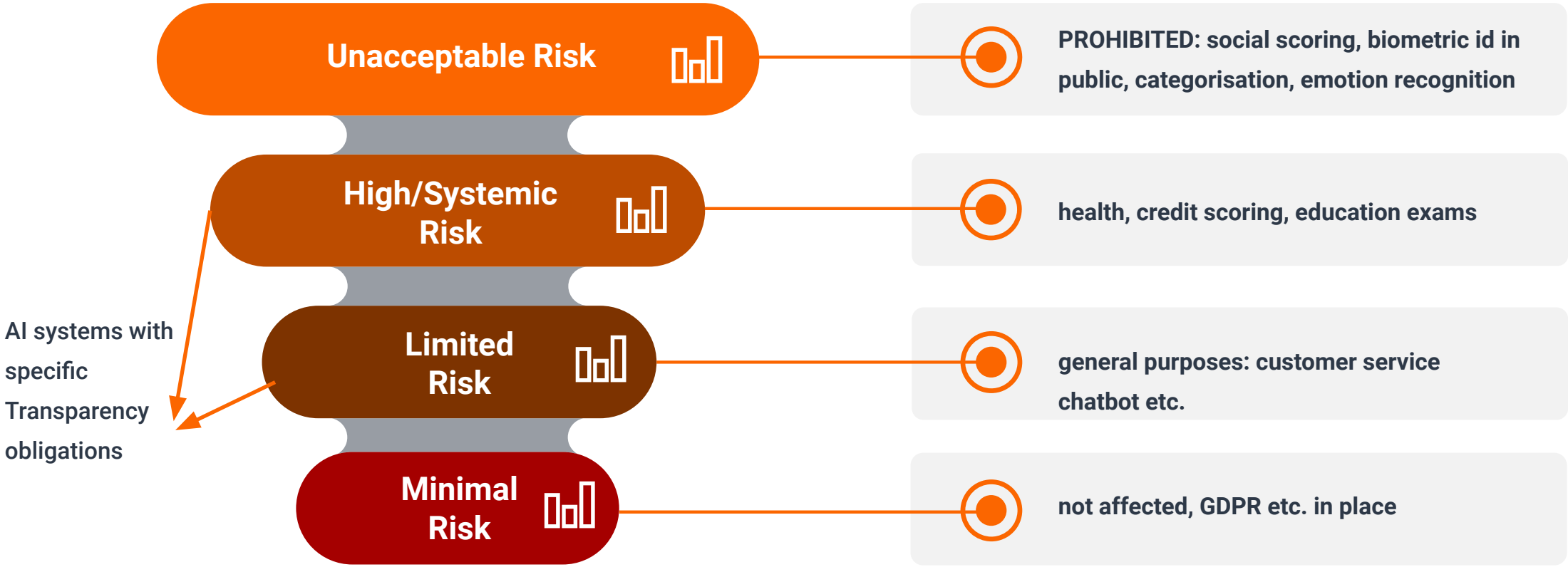
IEEE

Advancing Technology for Humanity

EU AI Act : overview

EU AI regulations are coming by 2024

AI Risk Categories



NOTE: it will take 6 (prohibited) to 24 (general purposes) months to enter into force

EU AI Act : impact in UK

EU AI regulations are coming by 2024

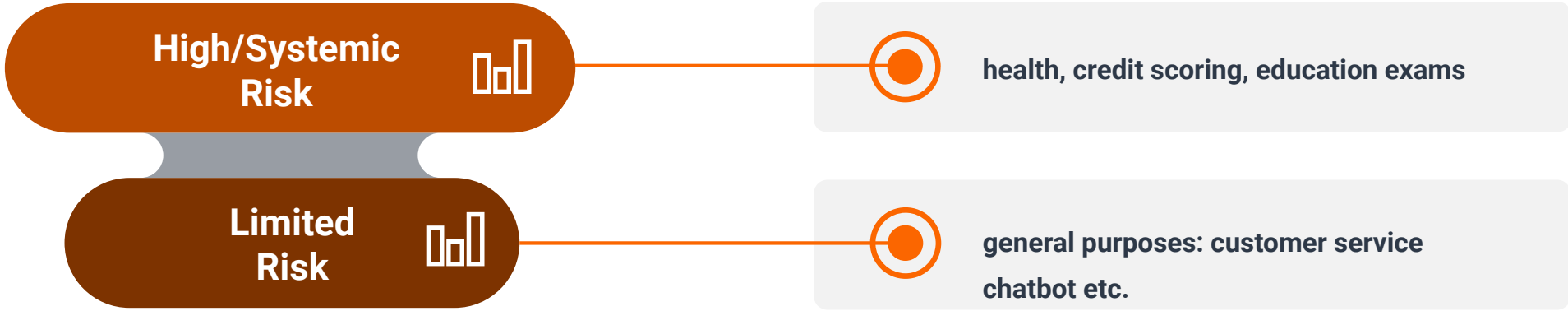
- Unless operating in EU, UK companies do not need to comply
- It may be on voluntary basis (marketing reasons etc.)
- UK has a 'vertical' approach to regulation: risk based, sector by sector by **extending** existing regulations
- UK regulators 'discretion': **recognition but not 'statutory duty' on five principles** – safety, security and robustness; appropriate transparency and explainability; fairness; accountability and governance; and contestability and redress.
- UK regulators impacted by AI "to publish an update outlining their strategic approach to AI by 30 April 2024" (finance by FCA etc.)
- If an AI supplier provides AI models to a sector (finance), it may now become subject to the sector regulator (FCA)

- UK has less AI regulations than EU but more 'discretion/ambiguity'
- In doubt, UK AI firms may be subject sector regulations more than in EU

BOTTOM LINE: a company should show it's behaving 'correctly', i.e. AI governance of some 'sort'

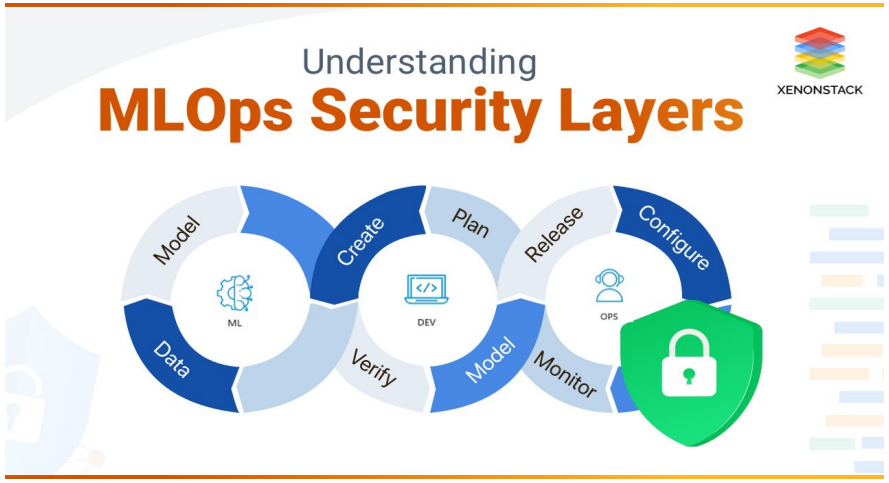
EU AI Act : what it means in practice

EU AI regulations are coming by 2024



- **Limited risk regulations (general purposes):**
- would apply in 12 months from Journal Publication (expected in few months)
- technical documentation available for clients of the AI system
- ‘summary’ of content and data used in training
- policy in place to respect copyright law

- **High risk regulations:**
- would apply in 24-36 months from Journal Publication (expected in few months)
- all requirements of limited risks
- AI model evaluation records
- AI model assessment and mitigation of risks
- management and response policy of incidents
- cybersecurity measures and adversarial testing



Impact on AI teams/MLOps

- AI teams should now follow a governance compliance framework (tbd)
- Simpler AI models will be favoured in production (less risk of incidents, etc.)
- Increase on training on governance and cybersecurity
- AI governance certifications (ISO, others) will be increasingly requested
- AI teams will ‘on purpose’ reduce quality of output to avoid incidents
- Insurance now cover both cyber and AI risks exposures

TECHNOLOGIES
Bring the future to humanity

Model Governance: what to do now

- Adopt data compliance roles into AI:

  DPO→AIPO

  data custodian → AI custodian

  data owner → AI owner

  data steward → AI steward

- Adopt a framework, EU or sector specific if UK:

  policy/procedures, risk assessments, incidents registers and reports

- If security and quality governance in place, add specific wording related to AI solutions or procedures

Certifications (ISO, etc.)

- Early days, ISO and IEEE main bodies
- some ISO 42001 policies just released , no certification yet
- AI definition same for ALL: ISO, IEEE, EU AI Act etc. (from OECD)
- AI certification has the ‘usual’ framework (quality, security, etc): policy/procedure, assessments, registers etc.
- If security and quality certification in place, add specific wording related to AI solutions or procedures

AI project running correctly

TECHNOLOGIES
Bring the future to humanity

AI Governance: Risk & Records

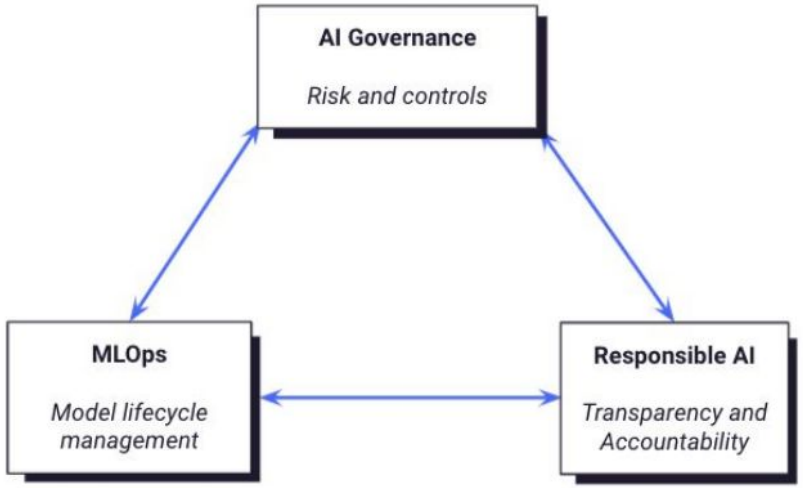
-cost/returns
-policy setting on AI behaviour
-define metrics to check
-define procedure for errors/hallucinations
-security compliance

MLOps

-run AI solution
-check technical performance
-bug fixing/improvements
-record incidents

Responsible AI team

-review AI behavior
-critical cases investigations



TECHNOLOGIES
Bring the future to humanity

Rules of Thumbs

what an executive should consider now

- the less explainable the AI the more governance you need → force the industry to use **as simple models as possible** (a good thing)
- check the **worst possible harm** of your AI application
- make sure **engineer in the team are 'champions'**
- check your **AI cybersecurity risk exposure** of your application
- mind the **AI policy like ISO 27001**: processes to monitor, investigate and records etc.
- Running an AI solution: **4-8% governance, 10-15% maintenance cost**

TECHNOLOGIES
Bring the future to humanity

Q&A

AI Newsletter

Thank you

Linkedin

andrea@aitechnologies.co